REMARKS

The Office Action mailed March 16, 2011 has been reviewed and carefully considered. The claims of the present application have not been amended herein. Claims 8, 14, 20 and 25 remain cancelled without prejudice. Claims 1-7, 9-13, 15-19, 21-24 and 26-27 are pending.

Claims 1-7, 9-13, 15-18, 21 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,904,522 to Benardeau et al. (hereinafter 'Benardeau') in view of U.S. Patent Application Publication No. 2002/0170053 to Peterka et al. (hereinafter 'Peterka') in further view of in further view of U.S. Patent Application Publication No. 2004/0064688 (hereinafter 'Jacobs') in further view of U.S. Patent Application Publication No. 2003/0126445 (hereinafter 'Wehrenberg'). Claims 19, 22 and 26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of Jacobs in further view of U.S. Patent Application Publication No. 2006/0212399 to Akiyama (hereinafter 'Akiyama'). Claims 23 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of Peterka in further view of Wehrenberg in view of Akiyama in further view of U.S. Patent No. 7,302,571 to Noble et al. (hereinafter 'Noble'). Claim 27 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Benardeau in view of Jacobs in further view of Akiyama in further view of U.S. Patent No. 7,797,552 (hereinafter 'Kahn'). The rejections are respectfully traversed.

The independent claims in the instant application are claims 1, 13, 19, 22, and 27.

It is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of claim 1:

> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said at least one slave digital terminal is adapted to receive a message from the transmitter instructing said at least one slave digital terminal to delete stored information necessary for accessing said protected digital data, to request, after receiving the message, from the master digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of claim 13:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal is adapted to receive a message from the transmitter instructing the digital terminal to delete stored information necessary for accessing said data and received by the second digital terminal to which it can be connected, to request, after receiving the message, from the second digital terminal new information necessary for accessing said protected digital data, and await the new information until an expiration of a predetermined deadline counted from a transmission of the request.

In support of the rejection, the Examiner has cited Benardeau as teaching a broadcast system with a master and slave that are connected to each other (see, e.g., Pending Office Action dated March 16, 2011 (hereinafter 'Office Action'), p. 3, para. 4 to p. 4, para. 1). Despite the Examiner's assertions otherwise, the Applicants respectfully submit that Benardeau fails to teach any of the features of the second clause of claim 1. For example, the Examiner maintains that the master terminal provides the slave terminal with information necessary for accessing protected digital data within a predeterminined deadline (see, e.g., Office Action, p. 3, para. 5 to p. 4, para.1). However, the purported predetermined deadline of Benardeau is the expiration time of the decryption key, which is not the same as a predetermined deadline by which a slave awaits new information from the time it makes a request for the new information. The Examiner has, at least partly, admitted this point (see, e.g., Office Action, p. 4, para. 1).

The Examiner has further admitted that Benardeau fails to teach the feature of instructing a digital terminal to delete stored information necessary for accessing protected digital data, as recited in claims 1 and 13 (see, e.g., Office Action, p. 4, para. 1 to p. 5, para. 2). To cure the deficiencies of Benardeau, the Examiner has cited Peterka (see, e.g., Office Action, p. 4, para. 2 to p. 5, para. 2). For example, the Examiner alleges that Peterka teaches sending "messages with the new key to delete the old ones." (Office Action, p.4, para. 2 to p. 5, para. 1). As described at length in the Applicants' previous Response, while the messages of Peterka comprise a new key, there is nothing in Peterka that teaches or fairly suggests deleting the old one. Consequently, there is no support for the Examiner's argument, at p. 5, para. 1 in the Office Action, that Peterka

teaches a delete message. The Examiner appears to admit this in the following paragraph (see Office Action, p. 5, para. 2).

To address the deficiencies of Benardeau and Peterka, the Examiner has introduced Jacobs as teaching the delete message feature as well as the request for new information necessary for accessing the protected digital data, as recited in claims 1 and 13. However, the Applicants respectfully submit that the Examiner's attempt at combining Peterka with other references to arrive at the deletion message and the request features is fundamentally flawed. Since Peterka's messages comprise the new key, which is the whole purpose of sending the message, the receiver then possesses the new key and there is no need for the receiver to seek it elsewhere. Specifically, the receiver will not request a new key after receiving the purported "delete message," as it includes the new key. The whole idea of combining Peterka with 'request' documents appears completely artificial and it is not something that one skilled in the art would do without improper hindsight reconstruction based on the teachings of the present application.

With regard to Jacobs, Jacobs teaches a secure packet-based data broadcasting architecture in which messages are sent from a CA system to clients. The messages may include commands to delete an entitlement and also INFO-messages that indicate the location of so-called IPECMs and IPEMMs.

A first problem with Jacobs is that the entitlements that may be deleted relate to the client's access profile, i.e. the services that the client is allowed to access (see, e.g., Jacobs, para. 0007, second sentence). If an entitlement is deleted, it is because the client no longer pays for the service. This means that the client should not have access to the service any longer. It follows that the client should not be able to obtain access without paying the required fee, but in this case the entitlement is added by using a command message (see, e.g., Jacobs, para. 0070).

However, as long as the client pays for the services, the access profile remains intact, which means that the client should receive the IPECMs that allow access to the service.

Essentially, in accordance with Jacobs, the entitlements are renewed, not deleted, as long as the client pays for the subscription and there is thus no need to request the information. If the client does not pay for the subscription, then he is not allowed the entitlement and there is thus no point in requesting it.

A second problem is that Jacobs does not, as the Examiner seems to suggest, teach that the client requests the new information. In fact, the purpose of the INFO message is to let the receiver know where the receiver should look for the IPEMMs and IPECMs. The INFO message essentially permits the receiver to identify which data stream sent by the service provider includes the message. For example, Jacobs teaches that the INFO message enables a receiver to "recognise" ECM and EMM packets by using information in their packet headers, which includes their associated IP address (see, e.g., Jacobs, para. 0077, lines 3-12). This can be quite important in an IP system, since information may arrive in many different ways and there can be substantial information that does not concern the receiver (such as multicasts to which it has not subscribed). Thus, Jacobs teaches that the head-end first informs the client as to where to "listen" for the information and then sends the information. Essentially, Jacobs merely adds to Benardeau-Peterka the INFO message that lets the clients know on which channel to listen for the key messages. This is substantially different from teaching that the receiver *requests* the key messages.

The Applicants also disagree with the Examiner's interpretation of Wehrenberg. For example, in support of the rejection of claims 1 and 13, the Examiner has cited paragraph 0085 of Wehrenberg as teaching that "a device that sends an encryption or authorization key can be timed by the requesting device and, if the requesting device does not receive the keys on time, it would stop its operations." (Office Action, p.2, para. 4). The Examiner further states that the other references clearly teach keys that are for accessing the content (Office Action, p.2, para. 4). In addition, the Examiner alleges that, in accordance with the broadest interpretation of Wehrenberg, if a device does not record content due to non-reception of a permission key, then the device will not access the content.

First, paragraph 0085 states that the recording **can** be stopped if the recorder does not receive the permission key on time. This is not the same as actually stopping recording. Second, Wehrenberg's keys are not for accessing the content; the permission key authorizes the recorder to record the content if the content is marked as 'record once.' In addition, while it is true that the device must access the content in order to record it, there is no teaching whatsoever in Wehrenberg that states that the device does not access content that it is not authorized to record. It is quite conceivable that the recorder continues to monitor received content that it cannot record. There is, in fact, no mention in Wehrenberg of a recorder that 'stops listening to

content.' Third, regardless of any purported teachings of the other references concerning keys that are for accessing content, Wehrenberg is directed to the use of permission keys that are directed to *recording* content; the permission keys are unrelated to enabling *access* to content. There is no teaching or suggestion in Wehrenberg that predetermined wait times should be applied to keys are that necessary for *accessing* content. Indeed, Wehrenberg's description teaches away from this application of wait times, as Wehrenberg explicitly states that a recipient is allowed to read the content despite not receiving the key (See, e.g., Wehrenberg, Abstract, lines 8-9).

As such, the Examiner's proposed combination fails to teach or render obvious at least the following features of claims 1 and 13: a) the transmission or reception of an instruction to delete stored information necessary for accessing protected digital data OR the subsequent request for new information and b) awaiting the new information necessary for accessing protected digital data until an expiration of a predetermined deadline counted from a transmission of the request. Accordingly, claims 1 and 13 are allowable over the cited references, taken singly or in any combination.

Additionally, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every feature of claim 19:

> System for receiving broadcast digital data, comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected data from a transmitter, the at least one slave digital terminal being connected to the master terminal by a link,
>
> wherein said slave digital terminal can access said received protected digital data only if information necessary for accessing said protected digital data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline,
>
> wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and

wherein the at least one slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Similar to claims 1 and 13 argued above, and now argued with respect to Claim 19, Benardeau does not teach or render obvious the feature of claim 19 relating to at least the recited "predetermined deadline."

Moreover, the cited references also fail to disclose the use of filter parameters, as recited in claim 19. For example, as described in the Applicants' previous Response, Benardeau teaches a system in which an ECM is sent from a slave to a master, which decrypts the ECM to extract the CW, re-encrypts the CW with a session key Ks and sends the re-encrypted CW to the slave. The slave decrypts the CW and employs the CW to descramble received broadcasts. Benardeau also mentions that the CWs may comprise copyright notification information, which may be used to prevent the slave from performing certain actions, such as recording or playing back the data.

In support of the rejection, the Examiner cites Jacobs and Akiyama as curing the deficiencies of Benardeau. With regard to Jacobs, contrary to the Examiner's assertions otherwise, the INFO-message merely informs the receiver about the data stream on which subsequent data will be transmitted so that the receiver knows where to 'listen' for the data, as described above. Moreover, as also discussed above, the Examiner's interpretation of 'deleting' is flawed, as it does not apply to situations in which receivers are entitled to receive data.

Further, the applicants also respectfully note that claim 19 recites a master digital terminal and a slave digital terminal that simultaneously receive protected data from a transmitter. However, a fair reading of Jacobs in combination with Benardeau gives one or the other of the following two possibilities: 1) The master in Benardeau sends an INFO-message to the slave to let it know how it will send the key information. In this case, there's no need for Jacobs' CA provider; 2) The slave obtains its information directly from the CA provider and there is no need for the master. In either case, the combination would not result in both a transmitter and a master digital terminal, as recited in claim 19.

With regard to other features of claim 19, the Examiner has noted that Benardeau and Jacobs do not teach that the digital terminal comprises filters that use filter parameters to extract the message containing the access entitlements (see, e.g., Office Action, p. 13, para. 3). To cure the deficiencies of Benardeau, the Examiner cites Akiyama.

As described in the Applicants' previous response, while Akiyama does indeed teach filters (see, e.g. 116 in Fig. 1), here, the filters extract desired packets from a multitude of packets for further treatment. However, it is unclear how the references can be combined to arrive at the features provided in claim 19.

For example, paragraphs 0120-0122 of Akiyama describe that content packets corresponding to the selected channel are extracted and sent to the descrambler 120, while common control packets are extracted by the filter and sent to a common control information decoder 117. Thus far, the filter merely checks the packet type and, for the content packets, checks that they correspond to the correct channel. Nothing here suggests that filtering is performed in any other way. Paras. 0125-0126 describe how the common control information decoder 117 checks a 'header' in the common control packet to decide which key to use to decrypt it. Even if this is considered filtering there is a verification that the proper key is detained. It would thus seem that Benardeau and Akiyama are incompatible, as there are no headers on the message including the encrypted CWs. In addition, paragraph 0160 describes essentially the same things as paragraphs 0125-0126. Further, paragraphs 0224-0227 describe exactly the same things as paragraphs 0125-0126, while paragraph 0227 details how individual control packets are treated; it is analogous with common control packets. Similarly, paragraphs 0237 and 0238 also describe exactly the same things.

As such, although Akiyama does describe filtering, Akiyama teaches examining the headers of the received messages, which is not possible in Benardeau, as there are no headers on the message including the encrypted CWs. Thus, the pertinence of Akiyama to the claim is unclear and it is also unclear how the reference can be combined with Benardeau. In any event, none of the cited references, taken singly or in combination, disclose or render obvious the features of: a) including in the information necessary for accessing said protected digital data *filter parameters* for *extracting* from the data stream received by the slave digital terminal a message containing *access entitlements* to the services for the slave digital terminal and b) at least one slave digital terminal that comprises filters that *use the filter parameters* to *extract the message containing the access entitlements*.

These points have already been presented to the Examiner and the Examiner has not addressed them in any way in the Office Action.

Accordingly, the Applicants respectfully request the withdrawal of the rejection of claim 19, as claim 19 is allowable over the cited combination for at least the preceding reasons.

Moreover, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of claim 22:

> A digital terminal intended to receive protected digital data from a transmitter generally simultaneously with a second digital terminal, wherein the digital terminal can access said received protected digital data only if information necessary for accessing said data and received by the second digital terminal to which it can be connected, is not received from this other terminal within a predetermined deadline,
>
> wherein the information necessary for accessing said protected digital data comprises filter parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal, and
>
> wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements.

Given the common limitations between claims 19 and 22 reproduced above, it is respectfully asserted that claim 22 is patentably distinct and non-obvious over the cited references for at least the same reasons set forth above with respect to claim 19. For example, at the least, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in claim 22 and argued above as well as the following feature recited in claim 22 and also essentially argued above "wherein the slave digital terminal comprises filters that use the filter parameters to extract the message containing the access entitlements."

Further, it is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest each and every limitation of claim 27:

> System for receiving broadcast digital data comprising:
>
> a master digital terminal and at least one slave digital terminal adapted to generally simultaneously receive protected digital data from a transmitter, the at

least one slave digital terminal being connected to the master terminal by a link,

wherein said slave digital terminal is adapted to receive from the transmitter a first part of an Entitlement Management message necessary for accessing said protected digital data, to receive from the master terminal a second part of the Entitlement Management Message necessary for accessing said protected digital data provided that it is received from the master digital terminal within a predetermined deadline, wherein the first part and the second part of the Entitlement Management Message enable accessing at least one decryption key for the protected digital data.

Preliminarily, it should be noted that it appears that the rejection of claim 27 is formally incorrect. For example, the paragraph bridging pages 16 and 17 mentions filter parameters (and further mention is found at the bottom of page 17), but the claim does not comprise such a feature. Even so, arguments already provided above regarding Benardeau, Jacobs and/or Akiyama still apply. For example, the cited references fail to show the claimed feature relating to the "predetermined deadline" recited in claim 27 and argued above, for example. However, claim 27 is patentable over the cited references for other reasons.

For example, with regard to the receipt of two parts of an Entitlement Management Message feature of claim 27, the Examiner admits that Benardeau, Jacobs and Akiyama do not teach that encryption keys are comprised of two parts and cites Kahn as teaching this feature. Kahn describes pairing a conditional access module (CAM) and one or more receivers so that the CAM only works when inserted into one of the specified receivers. This appears to be controlled through the use of a pairing key. However, even though Kahn mentions a second receiver, the pairing keys, etc., these aspects are directed to CAM-receiver interaction. Since the CAM and the receiver work together, i.e. they form a single working receiver, the CAM alone cannot be interpreted as a receiver (master or slave). The Examiner has also not explained how Kahn teaches that one part of an EMM is received from a master and another part from of the EMM is received from a transmitter, as recited in claim 27. Thus, the Applicants respectfully submit that claim 27 is patentably distinct and non-obvious over the cited references, as the references do not teach or render obvious at least the feature of receiving first and second parts of an EMM from a transmitter and a master terminal, respectively, as recited in claim 27.

Hence, none of the cited references, either taken singly or in any combination, teach or suggest all of the above-reproduced limitations of independent Claims 1, 13, 19, 22, and 27.

Accordingly, claims 1, 13, 19, 22, and 27 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above.

Claims 2-7, 9-12, 15, 17, 21, and 23-24 depend from claim 1 or a claim which itself is dependent from claim 1 and, thus, includes all the elements of claim 1. Claims 16 and 18 depend from claim 13 or a claim which itself is dependent from claim 13 and, thus, includes all the elements of claim 13. Claim 26 depends from claim 19 and, thus, includes all the elements of claim 19. Accordingly, claims 2-7, 9-12, 15, 17, 21, and 23-24 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to claim 1. Claims 16 and 18 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to claim 13, and claim 26 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to claim 19.

Thus, reconsideration of the rejection is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of March 16, 2011 be withdrawn, that pending claims 1-7, 9-13, 15-19, 21-24, and 26-27 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

No fee is believed due with regard to the filing of this amendment. However, if a fee is due, please charge Deposit Account No. 07-0832.

Respectfully submitted,

Philippe Leyendecker, et al.

By: /Paul P. Kiel/

Paul P. Kiel, Attorney for
Applicants
Registration No. 40,677
(609) 734-6815

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

Date: 6/16/11